SPECIAL FEATURE
JULY 2016
VOLUME 19 / ISSUE 2

System-Aware Cyber Security: A Systems Engineering Approach for Enhancing Cyber Security

Barry M. Horowitz, *University of Virginia*, bh8e@virginia.edu; and **D. Scott Lucero**, *Office of Secretary of Defense*, don.s.lucero.civ@mail.mil

ABSTRACT
This article highlights the importance of concurrently addressing process, people, and technology factors when conducting research related to new systems engineering concepts. In particular, an ongoing US Department of Defense-sponsored, University of Virginia-led cyber security research project is used as an example of how concurrent research activities provide value earlier in the technology design phase than otherwise would have occurred. The example project focuses on adding a new layer of protection for computer-controlled physical systems. Through concurrent efforts, the research team developed a better a protection approach, resulting in better prospects for transition into use.

INTRODUCTION

For the past several years, the US Department of Defense (DoD) sponsored a University of Virginia (UVa) research effort to investigate methods for bringing security engineering into the systems engineering trade space. The goal was to determine if there are design patterns with inherent resilience that would augment today's network and perimeter methods for securing systems. The research efforts led to development of "system-aware" cyber security, which refers to methods for enhancing the cyber security of physical systems, such as autonomous vehicles, automobiles, radars, turbines, and military weapons. System-aware cyber security adds a layer of security focused on detecting and deflecting attacks that have successfully penetrated a system's perimeter, either from outside attacks, or from supply chain or insider-initiated attacks (Under Secretary of Defense 2013).

System-aware cyber security relies on highly secured electronic sentinel(s) that monitor the protected system. Small, low power, prototype sentinels, including sensors, microprocessors, and communications devices, exist for a variety of systems. The sentinel protects critical functions and technologies by detecting illogical behavior in the control of a system, and restores the system to normal operation when possible.

As UVa developed and applied the methods, the research team discovered that transitioning systems engineering research into practice differs from a traditional technology transfer. In addition to technology development, we need new engineering methods to account for process and people, or human factors-related, transitions. The researchers found that prototype-based experimentation was effective for developing the technology as well as for developing needed new engineering processes. This article describes the system-aware cyber security technology, as well as the methods for transitioning systems engineering research into practice.

SYSTEM-AWARE CYBER SECURITY

To combat the threat posed by cyber attacks on cyber physical systems, a UVa-led research team proposed a system-aware, sentinel-based cyber security concept, complementing existing network and perimeter security solutions by adding an additional layer of defense (Jones et al. 2013; Jones and Horowitz 2012; Horowitz and Pierce 2013). The term "system-aware" indicates that the design of sentinels must directly account for how engineers design the system being protected and its operation, in contrast to network and perimeter security solutions.

The proposed defense approach is to prevent an adversary from compromising computer-controlled physical system(s) by ensuring the proper operation of the most critical subsystems and system functions, as identified by the owners and operators of the system being protected. Decision-making regarding which system functions to monitor and protect is a complex ***process*** topic (Jones et al., 2013). For example, the owners and operators of a surveillance system may decide to protect the operator interfaces that control important system behaviors, such as false alarm rate and probability of detection for a radar, whereas the owners and operators of a power plant may decide to protect the power generation subsystems, such as the turbine controller. The research revealed the need for analysis tools to evaluate alternative security solutions in a complex trade space involving risks, the criticality and vulnerability of the different system functions to protect, the attributes of various attack patterns, and the capability and cost of potential countermeasures. Furthermore, the selected defenses need to address the availability of alternative attacks

Table 1. Sample reusable design patterns

Design Pattern	Purpose
Diverse Redundancy	Post-attack restoration
Diverse Redundancy and Verifiable Voting	Attack deflection
Physical Configuration Hopping	Moving target defense
Virtual Configuration Hopping	Moving target defense
Data Consistency Checking	Data integrity and operator display protection
Parameter Assurance	Parameter-controlled software functions
Doctrinal Assurance Checking	Critical decisions

should the new defenses be employed, confirming that alternative, equally attractive attack paths do not remain available.

Using system-specific information capitalizes on one advantage that cyber security designers have over potential adversaries — in-depth knowledge of the system. System-specific countermeasures, however, limit the reusability of such defense solutions. Furthermore, these additional defenses will incur costs and could introduce new vulnerabilities. Reusable design patterns provide an important mechanism for developing defenses while containing costs. See Table 1 for sample reusable design patterns.

Evaluating various trades and design patterns drove the research team to select a small, highly secure sentinel design pattern involving a moving target solution, thereby reducing risk of the sentinel itself becoming the target of cyber attacks. The research team found that the cost for secure monitoring via the sentinel would be far less than for directly securing the system. In addition, investments in directly securing the system could be lost through vulnerabilities introduced when enhancing the system's functionality. Keeping the sentinel small, static, and secure reduces this risk, as well as the implementation costs.

The sentinel defense-in-depth approach required development and integration of ***technology*** for implementing the sentinel design pattern, and integration concepts for combining multiple sentinels to protect against distributed cyber attacks. In addition, the researchers had to address ***human factors***, in other words, operational processes of human operators, to enable a sentinel to reconfigure a compromised system to allow near-continuous operation. The research demonstrated that concurrent activities are needed to address the three dimensions of process, people, and technology in systems engineering in order to more rapidly transition the research into practice. The research relied on the use of prototypes to investigate these dimensions of systems engineering, as described in the following paragraphs.

TRANSITIONING SYSTEMS ENGINEERING RESEARCH THROUGH USE OF PROTOTYPES

Engineers use prototypes to improve technologies and increase the functionality of systems. These prototyping approaches become increasingly important as:

- The cost of advanced technologies has come down
- Accessibility of open source software, design and evaluation tools, and on-line laboratories increases (Hencke 2014)
- Access to technology infrastructures, such as Global Positioning System (GPS) navigation, cloud computing, and the Internet, continues to increase
- Use of open standards that support systems integration continues to increase, such as Controller Area Network (CAN BUS) networks on cars and Ethernet networks on unmanned aerial vehicles (UAVs).

The research team conducted live experiments using prototype sentinels protecting currently employed physical systems, for example, UAV-based surveillance systems, police cars, 3-D printers. As the team performed the sentinel technology research, they realized they would have to change the typical practice of systems engineers for the system-aware design patterns to take root. While the benefits of improved technology are often obvious, the benefits of improved design processes are not as readily apparent. A prototyping environment can be used to develop improved engineering processes, as well as technologies. For systems engineering research to transition to broader use, working through the process and human factors issues may be as important to improve system designs as the specific technologies themselves.

SYSTEM-AWARE RESEARCH EFFORTS AND RESULTS

The system-aware cyber security research team developed prototypes in five application areas. Following is a description of one of the efforts, an autonomous surveillance system onboard a UAV, addressing the process, people, and technology elements of the research. The other research application areas have yielded complementary findings regarding these three elements of research.

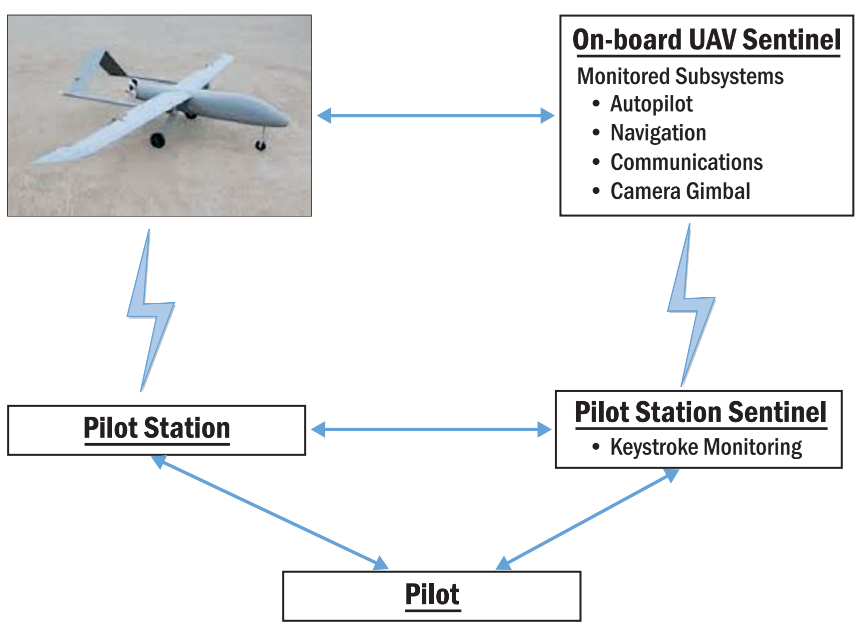

Figure 1. Operational configuration for cyber security evaluation

Technology

A UVa-led research team and Georgia Tech Research Institute (GTRI) explored a number of cyber attacks that would have a significant impact on the surveillance mission of a UAV. One of several attack scenarios involved changing aircraft navigation system waypoints, either through a communicated command or an onboard embedded attack that could be externally initiated or self-triggered, for instance, based on the aircraft's location. The prototype used an Outlaw aircraft, with a 16-foot wingspan and 40-pound payload, collecting video information over a designated geographical surveillance area (Figure 1).

Experiments included in-flight cyber attacks and corresponding sentinel-derived responses, which required development of new flight-safety testing procedures (Heiges, et al., 2015). The research team designed ground and aircraft-based sentinels to:

a) Detect waypoint changes on the aircraft
b) Discover whether or not a command to change a waypoint came to the aircraft
c) Determine whether or not an operator keyboard entry to send such a command had occurred
d) Integrate this information to determine whether or not the waypoint change system was operating as designed
e) Communicate illogical behaviors to designated locations
f) Restore the modified waypoint if commanded to do so.

The research team reviewed the design patterns and chose several to develop the airborne sentinel, including triple diverse redundancy for individual system components, and a hot shadowing operation using three different cyber attack detection methods. Comparing the results of these three methods would discover a cyber attack that corrupted any one of these diverse implementations. In addition, the research team chose a moving target cyber security defense, where the specific detection method that was in control was dynamically changed every few seconds. The technical performance evaluations were positive. Only a few hundred lines of software were needed to implement the individual defenses. The research team is currently investigating the cost and scalability of the methods for different types of systems to help address process and human factors concerns.

Process

When this research effort started, the UVa-GTRI research team manually derived the specific UAV functions to defend in the prototyping effort. The team evaluated the trade space using their knowledge of surveillance missions, autopilot design, camera gimbal control systems and navigation systems, as well as various cyber attack methods. The team also obtained information from the vendors of the various subsystems on the aircraft.

As the research team began using the security engineering methods, they changed the priorities of what to defend based on the ability to develop specific defenses, the ability of adversaries to respond to those defenses, and specific attacks that could be directed at the sentinels. For example, the research team wanted to defend against a supply chain-based attack on the aircraft's GPS navigation system using GPS receivers from different manufacturers to detect and respond to this type of attack. The costs of this diverse redundancy, however, were too high compared with defenses for different but equally concerning attacks. Later in the design process, the research team discovered that the aircraft's camera gimbal system included a diversely manufactured GPS receiver. While this late discovery enabled the originally desired sentinel technology to be implemented within desired economical constraints, it is clear that design decisions need to be based on more accurate and complete system design information.

Based on this emergent result, the research team investigated use of the Systems Modeling Language (SysML), an open standard system modeling language, to evaluate the system to be protected. The team also investigated using attack tree tools in conjunction with SysML to develop attack scenarios. These efforts helped the team identify opportunities for engineers to red-team their designs early in development, rather than waiting for red teams to attack systems during the verification process. One of the goals of this research was to bring security requirements into the systems engineering trade space. Engineering tools have a great potential to help systems engineers make these design decisions during the development process.

Human Factors

As part of the UAV-related research effort, the UVa research team partnered with the MITRE Corporation to develop a desktop simulation to see how operators would respond to sentinel detections of cyber attacks and suggested options to reconfigure the system. While the operators found great value in the sentinel's information on detected attacks, results revealed that certain operators:

- Would terminate a mission because they were concerned that the detected attack did not have additional, yet to emerge, elements
- Would like to talk with a cybersecurity expert to get technical support to improve mission decisions
- Were concerned that the sentinel was the target of the "detected" cyber attack, causing operators to make ill-informed decisions.

This unanticipated outcome identified the need for operator training regarding responses to cyber attacks. In addition, the researchers noted that actual events had occurred with consequences similar to the experimental cyber attacks, and were categorized as "cause unknown and consequences cannot be reproduced." Training for unusual events resulting from unprecedented, zero-day attacks will be a critical challenge. Based upon these outcomes, the Air Force Institute of Technology (AFIT) started working with UVa's system-aware research team to conduct human factors research, building on Air Force Research Laboratory research on operator suspicion and its impact on operator performance in working in advanced automation environments. Human factors experiments with remotely piloted systems are scheduled to start, using cyber attack scenarios as well as system-aware technology.

CONCLUSION

The system-aware design concept is based upon a system architecture approach that uses a new layer of cybersecurity to enhance the security of physical systems. Early technology-based research uncovered emergent issues that highlighted critical process and human factors concerns that early adopters would need to consider; namely the need for design tools and a well-defined decision process for navigating the cybersecurity trade space, and the need to develop well-defined operator response procedures for detected attacks.

In addition, the researchers identified opportunities for systems engineers to evaluate their designs in a prototyping environment, not only to improve the technology, but also to improve the process for applying the technology. Addressing process, people, and technology concerns will be essential for transitioning this system-aware cyber security research into widespread practice. Continuing research should help address all of these areas of concern, based on lessons learned from early adopters as well as insights from the academic community.

ACKNOWLEDGMENTS

This material is based upon work supported, in whole or in part, by the US Department of Defense through the

> continued on page 42

Crane continued from page 38

and the larger the scale, the smarter an agile system becomes. For organizations to manage risks effectively and proactively within a risk appetite, they must move to a dynamic, automated, agile risk management capability.

We have developed a distributed software solution, based on an Autonomous Networked Topology Security (ANTS™) system that enables the sharing of "nervousness" information about immediate risks. This provides an organic, self-organizing system that empowers every element to contribute individually to the collective security of your enterprise ecosystem. The result is an agile defense that enables organizations to take protective defensive actions automatically when risk exceeds an organization's defined cyber risk appetite. ■

REFERENCES

- Amato, P. 2013. From Ants to Civilization: A Biologist's Take on What Makes Us Tick. *Contemporary Sociology* 42 (3) (May 2013): 364-7.
- Dove, R. 2010. "Pattern Qualifications and Examples of Next-Generation Agile System-Security Strategies." Paper presented at 2010 IEEE International Carnahan Conference on Security Technology (ICCST), San Jose, US-CA, 5-8 October.
- Federal Trade Commission. 2015. FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks. Lanham, US-MD: Federal Information & News Dispatch, Inc.
- Heath, B. L. and R. R. Hill. 2010. Some Insights into the Emergence of Agent-Based Modeling. *Journal of Simulation* 4 (3) (print): 163-9.
- IMS Research. 2010. Internet Connected Devices About to Pass the 5 Billion Milestone.
- Jericho Forum. 2007. White Paper Business Rationale for De-Perimeterisation.
- Macal, C. M. and M. J. North. 2007. *Managing Business Complexity: Discovering Strategic Solutions with Agent-Based Modeling and Simulation*. Oxford, US-NY: Oxford University Press.
- NIST. 2014. Cybersecurity Framework. Lanham, US-MD: Federal Information & News Dispatch, Inc.
- Rittenberg, L. and F. Martens. 2012. Enterprise Risk Management – Understanding and Communicating Risk Appetite. *Thought Leadership in ERM*. The Committee of Sponsoring Organizations of the Treadway Commission (COSO).
- US Treasury Department. 2015. Cybersecurity: FFIEC Cybersecurity Assessment Tool. Lanham, US-MD: Federal Information & News Dispatch, Inc.
- Verizon Enterprise Solutions. 2015. *Data Breach Investigations Report*.

ABOUT THE AUTHOR

Dr. Earl Crane is the co-founder and the chief executive officer of Emergent Network Defense, Inc. (END). Dr. Crane has advised the President of the United States as the director for federal cyber security policy on the White House National Security Council, Wall Street executives, and multiple Fortune 100 corporations on their cyber defensive strategies. Dr. Crane led the implementation of the US Department of Homeland Security's information security strategy, and has taught hundreds of cyber security masters students and executives through Carnegie Mellon's Heinz College and chief information officer (CISO) certificate program. He earned his PhD from George Washington University, a Masters of Information System Management at Carnegie Mellon University and a BS in mechanical engineering at Carnegie Mellon University. He is helping organizations engage in cyber security discussions with impact to their real-world challenges and enable executives to reduce their corporate cyber security risk.

Horowitz and Lucero continued from page 41

Systems Engineering Research Center (SERC) under Contracts HQ0034-13-0004. The SERC is a federally funded University Affiliated Research Center managed by Stevens Institute of Technology, Hoboken, NJ, USA. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the US Department of Defense.

GTRI, AFIT and MITRE Corporation provided significant contributions to the research activities described in this article.

REFERENCES

- Heiges, M., R. Bever, and K. Carnahan. 2015. "How to Safely Flight Test a UAV Subject to Cyber-Attacks." Presentation at SCI-269 Symposium, NATO Science and Technology Organization (STO).
- Hencke, R. B. 2014. "Prototyping, Increasing the Pace of Innovation." *Defense Acquisition, Technology, and Logistics*. July-August
- Horowitz, B., and K. Pierce. 2013. "Application of Dynamic System Models and State Estimation Technology to the Cyber Security of Physical Systems." *Systems Engineering*. 16 (4): 401-412.
- Jones, R. A., and B. M. Horowitz. 2012. "System-Aware Cyber Security Architecture." *Systems Engineering* Vol. 15 (2): 224-240.
- Jones, R. A., B. A. Luckett, P. A. Beling, and B. M. Horowitz. 2013. "Architectural Scoring Framework for the Creation and Evaluation of System-Aware Cyber Security Solutions." *Environment Systems and Decisions* 33 (3): 341-361.
- Under Secretary of Defense for Acquisition, Technology, and Logistics. 2013. Defense Science Board Task Force on Resilient Military Systems and the Advanced Cyber Threat. Washington, US-DC: US Department of Defense.

ABOUT THE AUTHORS

Dr. Barry Horowitz is a professor of systems and information engineering and chair of the department at the University of Virginia. He was elected into the National Academy of Engineering in 1996. Previously, he held a variety of positions at the MITRE Corporation, including president and chief executive officer.

Scott Lucero is the deputy director of strategic initiatives in the US Office of the Deputy Assistant Secretary of Defense (Systems Engineering). He is the program manager of the Systems Engineering Research Center (SERC), a consortium of the top US universities performing research in systems engineering.